REMARKS

In the Official Action mailed **5 May 2005**, the Examiner reviewed claims 1-5, 7-13, 15-21, and 23-48. Claims 1-5, 7-13, 15-21, and 23-48 were rejected under 35 U.S.C. §103(a) as being unpatentable over O'Flaherty et al (USPN 6,275,824, hereinafter "O'Flaherty") in view of Sweet et al (USPub 2002/0031230, hereinafter "Sweet").

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 9, 17, 25, 33, and 41 were rejected as being unpatentable over O'Flaherty in view of Sweet.

Applicant respectfully points out that both O'Flaherty and Sweet teach away from the present invention.

In the invention of O'Flaherty, **a user or an administrator can** determine the security settings of sensitive information. Specifically, a user can "*permit the dissemination of sensitive data*" (see O'Flaherty, col. 7, lines 37-45). Furthermore, a database administrator can set up views so that "*all columns of personal information are hidden*" (see O'Flaherty, col. 8, lines 25-29). In other words, the invention of O'Flaherty allows users and/or database administrators to determine security settings of sensitive (or personal) information.

In contrast, in the present invention, **an administrator cannot** determine the security settings of sensitive information. Specifically, only security officers can "*perform administrative functions for ... sensitive information*" (see page 7, lines 9-11). In fact, the present invention *explicitly* states that database administrators are ***not allowed*** to perform administrative functions on sensitive information (see page 10, lines 1-3). It will be obvious to one skilled in the art that determining the security setting is an administrative function. Hence, the present invention explicitly disallows users and/or database administrators to determine security settings of sensitive information.

Additionally, in the invention of Sweet, an **administrator is allowed** to change a sensitive user's security profile. Responsibilities of administrators include "*assigning, distributing and updating **member** security profiles*" (see Sweet, [0110]). Particularly, an administrator can "*modify the security profile*" (see Sweet, [0206], lines 2-3). Moreover, "*administrators can change **anyone's** status immediately*" (see Sweet, paragraph [0061], lines 8-9). It will be obvious to one skilled in the art that terms like "member" and "anyone" are interpreted broadly, and hence can be interpreted to refer to sensitive users. Thus, the invention of Sweet allows an administrator to change a sensitive user's security profile.

In contrast, in the present invention, **an administrator is not allowed** to change a sensitive user's security profile. Specifically, database administrators "*cannot change any attributes attached to sensitive users*" (see page 8, lines 12-13). Note that the broad term "attribute" can refer to security attributes that make up a security profile. Hence, the present invention *explicitly* disallows an administrator to change a sensitive user's security profile.

Note that it is critically important to disallow an administrator to perform administrative functions on sensitive data or to change attributes attached to sensitive users. Otherwise, "*a rogue administrator can potentially become a sensitive user, and can thereby obtain access to sensitive objects indirectly*" (see page 8, lines 15-17).

Furthermore, note that methods and systems for preventing rogue administrators from compromising security are not obvious. This is because they involve the complex steps and components described in FIGs. 1, 3, and 4.

Accordingly, Applicant has amended independent claims 1, 9, 17, 25, 33, and 41 to clarify that (a) the database system has administrators and security officers, (b) a security officer can perform administrative function on sensitive objects, (c) an administrator cannot perform administrative functions on sensitive objects, (d) an administrator cannot become a sensitive user and thereby obtain access to sensitive objects indirectly, and (e) a command to perform an

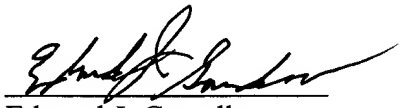
administrative function on a sensitive object is disallowed if it is received from an administrator. These amendments find support on page 7, lines 9-11, page 10, lines 1-3, and page 8, lines 12-13 of the instant application.

Hence, Applicant respectfully submits that independent claims 1, 9, 17, 25, 33, and 41 as presented are in condition for allowance. Applicant also submits that claims 2-5 and 7-8, which depend upon claim 1, claims 10-13 and 15-16, which depend upon claim 9, claims 18-21 and 23-24, which depend upon claim 17, claims 26-32, which depend upon claim 25, claims 34-40, which depend upon claim 33, and claims 42-48, which depend upon claim 41, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 

Edward J. Grundler
Registration No. 47,615

Date: 17 June, 2005

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616-7759
Tel: (530) 759-1663
FAX: (530) 759-1665